GDPR – What Do You Need to Know?

1 Introduction

As the leading global provider of Talent Assessment solutions, we take our obligations to ensure the highest level of protection over the personal data you entrust to us very seriously. Maintaining compliance with applicable data protection legislation continues to be a core business priority.

This statement provides you information regarding our compliance with, and our programs to support your compliance with, the General Data Protection Regulation (GDPR) which took effect on 25 May 2018. In our role as data processor we have a demonstrated track record of data security and sound practices.

We are committed to being GDPR compliant, as further detailed in Section 3 and are on a continuous improvement journey.

2 What Is the GDPR and What Does It Mean for You?

The GDPR and the United Kingdom's Data Protection Act 2018 are significant changes to the EU and UK data protection framework with several key changes that impacted our services and our clients:

- **Accountability:** The new principle of accountability under the GDPR requires organisations to more explicitly demonstrate compliance with the GDPR principles.
- **Expanded Individual rights:** Individual rights (rights of access, rectification, to object to data processing and to restrict processing), adding the right to be erased and the right to data portability for each data subject.
- **Governance framework:** Intertwined with the accountability principle, is the requirement on data controllers and data processors to implement appropriate technical and organisational measures and to demonstrate any processing of personal data is in compliance with the GDPR.
- **Fines**: EU Member State Supervisory Authorities and the UK's Information Commissioner's Office (who are responsible for enforcing the GDPR) can impose fines of up to 4% of global turnover or 20,000,000 Euros, whichever is the higher, for breaches of the GDPR.

3 Why Work With Us

We prioritise data security: We understand and have always taken our security obligations seriously, long before the GDPR. Our commitment to security is demonstrated by our on-going certification programs that have been in place for many years. In particular, we have developed and implemented an ISO 27001 certified Information Security Management System for over 10 years running. Additionally, we have obtained ISO 22301 certification for our Business Continuity Practices and we have ISO 20000 certifications for our ability to professionally maintain, support and manage our IT services using best practices.

We have taken all required actions. We took the following actions to further enhance our robust data protection systems to comply with the GDPR.

- **Upgraded policies and procedures:** As part of our GDPR compliance strategy we reviewed and upgraded existing policies and procedures to ensure that we comply with the GDPR. All our staff and key individuals are continually trained on these policies for our compliance and to offer you assistance with your compliance efforts.
- **Upgraded data protection notice:** Our current data protection notice presented to candidates when they take an assessment complies with GDPR requirements.
- **Upgraded data processor agreements:** We updated our data processor agreements with our clients to include provisions to complies with GDPR requirements.
- **Privacy by design and default:** We are committed to facilitating our clients' data protection governance strategy, including the new prescribed obligations of privacy by design and default. Privacy by design requires organisations to take appropriate measures to integrate the GDPR's data protection principles into their operations whilst taking into account cost, context and risk. Privacy by default requires organisations, as a default position, to take appropriate technical and organisational measures to minimise data usage for each purposes for which is it collected.
- **Personal data breach notification:** Under the GDPR you have an obligation to notify the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of a personal data breach. In the event we become aware of a breach affecting your personal data, we will notify you without undue delay in no more than 48 hours and assist you in complying with your GDPR obligations by providing you the required information related to the personal data breach in a timely manner.
- **Privacy impact assessments:** We will facilitate your compliance with the GDPR obligations by assisting you with privacy impact assessments to identify and minimise the risk of non-compliance.
- **GDPR Compliance monitoring:** We will continue to regularly review and audit the security of our services and our compliance with our GDPR policies and procedures.
- **Training:** Continuing on from our long-standing data protection training program, we will continue to train our staff globally on data protection requirements,
- including the GDPR, as part of our ISO 27001 certification. Additionally, we perform extensive training to key individuals as required under the GDPR.
- **Maintaining records of processing:** As required by the GDPR, in our role as data processor, we maintain a record of our processing activities for each type of data processing we carry out.
- **Individual rights assessment:** Under GDPR you, as data controller, are obliged to facilitate the exercise of each data subject's rights. As your data processor, we have set out below the ways in which our systems and processes can support you in meeting your obligations to the data subjects:

GDPR Article	Compliance
Article 13 **The right to be informed**	Our assessment platform includes a data protection notice which individuals are presented with prior to taking the assessment. This notice provides information to the individual about the collection and processing that we perform, in accordance with data protection legislation requirements. As the assessment makes up one part of an overall recruitment process, (and the assessment is generally not your first point of candidate data collection) the Article 13 notice requirements may also need to be satisfied earlier than our assessment platform. You may employ several different methods, such as your careers website, an online application form, or applicant tracking system to receive initial applications, and collect other personal information e.g. CV or résumé information, residential address etc. In each of these systems, a data protection notice that addresses the full recruitment cycle would be required at the point of data collection. You would need to seek independent legal advice on your compliance obligations under Article 13 GDPR.
Article 15 - 18 **The right;** • **of access** • **to rectification** • **to erase** • **to restrict processing**	A candidate's request to access, correct, delete or restrict processing of data should be directed to you, as the data controller. We occasionally receive requests directly from candidates to delete their information, or to provide access to their assessment results. We redirect these candidate requests back to as the data controller. We then provide support and information to you as you require to meet your obligation to the candidate. If we receive such a request directly from you as our client, we already have processes in place to carry out that request, whether that is promptly responding to a data subject access request, or a request for deletion of data. Clients often ask "how long do you retain data?" As a data processor, we retain data in accordance with our client agreements, meaning we delete data following a request from you, our clients. As part of our GDPR compliance strategy we made improvements within our platform to build in increased automation and efficiencies into our data deletion processes.
Article 20 **The right to data portability**	The right to data portability only applies: · to personal data an individual (i.e. a candidate) has provided to our clients as the data controller; · where the processing is based on the individual's consent or for the performance of a contract; and · when processing is carried out by automated means (it does not apply to paper records). Given the context of the products and services that we offer, we see this right as being quite closely related to the right to access as noted above and we would direct any such requests back to you as the data controller, and then assist in your decisions to comply. The information that is collected directly from the individual is limited, and therefore providing this in a "structured, commonly used, machine-readable and interoperable format" can be easily done on a case by case basis. It would be up to you as the data controller to determine the extent of the information that you would make available under this right.

GDPR Article	Compliance
Article 21 **The right to object**	A candidate may have a right to object to the processing of their personal data if you, as the data controller, rely on legitimate interests as the legal basis for processing. Candidates are free to choose whether to take an assessment or not. If they object to the processing of data, an individual can simply close out of the assessment and we will not perform any further processing. If the candidate objects after they have started an assessment, this will become a right to deletion under Article 15.
Article 22 **Rights in relation to automated decision making and profiling**	The GDPR provides a right for individuals not to be subject to any automated decisions unless certain exemptions apply. Our clients often use our services to aid in making decisions as to whether to offer employment or a promotion to an individual. Our best practice guidelines recommend that our assessments should be used as part of an overall evaluation and should not be relied upon as the sole basis for any employment related decisions. For any other use of our assessments we would advise you to seek independent legal advice on your compliance obligations under Article 22 GDPR. As the data controller, if you inform us you intend to use our assessment as part of an automated decision, we can follow your instructions regarding your approach to any permitted exception, such as sufficient notification to individuals that they may be subject to an automated decision.

We comply with international transfer rules: In accordance with our current practice we will continue to ensure we do not transfer data outside of the EEA without an appropriate data transfer structure in place. Currently, we have EU Standard Contractual Clauses ("Model Clauses") in effect for transfers outside of the EEA to ensure adequate levels of protection as permitted by the European Commission.

We are also updating our policies and procedures in anticipation of the withdrawal of the United Kingdom from the European Union. Regardless of the outcome of Brexit, SHL is still committed to the GDPR and we are currently evaluating possible options with respect to the transfer of data between the UK and the EEA.

We rely on self- certification under the EU-US Privacy Shield for transfers to the US. Privacy Shield is a self-certification programme under which organisations can register with and confirm they meet specific privacy requirements. The Privacy Shield is not expressly referenced in the GDPR, but it is recognised by the European Commission as providing adequate protection. We will continue to monitor any proposed changed to Privacy Shield and Model Clauses following the GDPR and ensure we upgrade our agreements and Privacy Shield certification as required.

Data protection agreements: We regularly enter into data protection agreements with our clients as required. Please work with your sales representative to contact us to update or implement the EU Standard Contractual Clauses or other statutory agreement to meet your requirements.

If you have any further questions please either speak to your account manager or email **data.questions@shl.com.**